REMARKS

In the final Office Action mailed November 27, 2009 the Office noted that claims 1-9 were pending and rejected claims 1-9. In this amendment claim 1 has been amended, no claims have been canceled, and, thus, in view of the foregoing claims 1-9 remain pending for reconsideration which is requested. No new matter has been added. The Office's rejections and objections are traversed below.

REJECTIONS under 35 U.S.C. § 102

Claims 1-5, 7 and 8 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Shimizu, JP 10-154976. The Applicant respectfully disagrees and traverses the rejection with an argument and amendment.

The Applicant has amended claim 1 to recite "method of making an electronic entity with encrypted access secure when said electronic entity executing a cryptographic algorithm consisting in applying to an input message a succession of groups of operations known as "rounds" involving a series of respective sub-keys produced successively by an iterative process starting from an initial key K, the method comprises performing steps of said iterative process so as to obtain a result of an iterative ***intermediate*** step." Support for the amendment may be found, for example, in the rest of claim 1. The Applicant submits that no new matter is believed to have been added by the amendment of

claim 1. The Applicant further submits that the previous wording of the claims was an obvious error and that no further search burden is placed on the Office and that the amendment should be entered as of right.

Shimizu discusses repeating a cryptographic algorithm in order to check whether the results of each implementation of the algorithm are identical (see comparison parts in ¶ 0073 of Shimizu) in order to detect a malfunction (supposed to come from a fault attack) and to refrain from outputting the result if a malfunction is detected (end of ¶ 0073).

The Applicant also brings to the attention of the Office, in the IDS of November 2, 2009, a partial translation of Shimizu was provided which more accurately translates the document than the machine translation relied on by the Office.

Shimizu fails to disclose checking the correct operation of the key extension process, as claimed. This is made clear in the Japanese Office Action, filed in the IDS of November 2, 2009, the Japanese Examiner relying on Shimizu as read in the Examiner's native language.

Furthermore, as noted above, Shimizu teaches comparing the results of a round function, i.e. the encrypted data, as explicitly mentioned in ¶ 0073, whatever the fault attack considered. This is because one of ordinary skill in the art naturally considers that checking the result of the whole algorithm (or part of the algorithm) would be sufficient to

detect any error caused within the whole process of the algorithm (or the concerned part of the algorithm).

One of ordinary skill in the art would therefore not have stored, reiterated and compared the results of a key extension process, as Shimizu teaches to compare the encrypted message resulting from the whole process, which seemed logically to be sufficient to detect a fault attack in any part of the preceding process leading to this encrypted message.

Thus, Shimizu fails to disclose "storing in said electronic entity said result of said intermediate step, repeating at least some of the steps of said iterative process until a result is recalculated corresponding to the result that has been stored, comparing the value of said stored result to the value of the corresponding recalculated result," as in claim 1.

Thus, for at least the reasons discussed above, claim 1 and the claims dependent therefrom are not anticipated by Shimizu.

Withdrawal of the rejections is respectfully requested.

REJECTIONS under 35 U.S.C. § 103

Claims 6 and 9 stand rejected under 35 U.S.C. § 103(a) as being obvious over Shimizu. The Applicant respectfully disagrees and traverses the rejection with an argument.

For at least the reasons discussed above with respect to the anticipation rejection, Shimizu fails to render obvious

the features of claims 6 and 9.

Withdrawal of the rejection is respectfully requested.

SUMMARY

It is submitted that the claims satisfy the requirements of 35 U.S.C. §§ 102 and 103. It is also submitted that claims 1-9 continue to be allowable. It is further submitted that the claims are not taught, disclosed or suggested by the prior art. The claims are therefore in a condition suitable for allowance. An early Notice of Allowance is requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/James J. Livingston, Jr./
James J. Livingston, Jr.
Reg.No. 55,394
209 Madison St, Suite 500
Alexandria, VA 22314
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

JJL/fb